Optimizing Investments in Security Countermeasures: A Practical Tool for Fixed Budgets

Jonathan Caulkins – Carnegie Mellon University [vita[1]]
Eric Hough – SPAWAR [vita[2]]
Nancy R. Mead – Software Engineering Institute [vita[3]]
Hassan Osman – Ernst & Young LLP [vita[4]]

2007-9-11 L2 / L, M[5]

Software engineers and businesses must make the difficult decision of how much of their budget to spend on software security mitigation for the applications and networks on which they depend. This article introduces a novel method of optimizing using integer programming (IP), the combination of security countermeasures to implement to maximize system security under fixed resources. The steps in the method and recent results with a case study client are described.

This article has been published in the September/October 2007 issue of *IEEE Security & Privacy* and is available for download[6] under Additional Resources.

Published by the IEEE Computer Society

1. http://buildsecurityin.us-cert.gov/bsi/about_us/authors/606-BSI.html (Caulkins, Jonathan)
2. http://buildsecurityin.us-cert.gov/bsi/about_us/authors/635-BSI.html (Hough, Eric D.)
3. http://buildsecurityin.us-cert.gov/bsi/about_us/authors/230-BSI.html (Mead, Nancy)
4. http://buildsecurityin.us-cert.gov/bsi/about_us/authors/637-BSI.html (Osman, Hassan)
6. http://buildsecurityin.us-cert.gov/bsi/resources/articles/904-BSI.html (Optimizing Investments in Security Countermeasures)